#6

In the United States Patent and Trademark Office

Serial Number: 09/081,872
Appn. Filed: 05/20/98
Applicant(s): John H. Messing
Appn. Title: Electronic Signature Program
Examiner: Douglas J. Meislahn
Group Art Unit: 2767

Mailed: December 28, 2000

At: Tucson, Arizona

Substitute Specification

Assistant Commissioner for Patents
Washington, District of Columbia 20231

Sir:

In response to the Office Action mailed September 28, 2000, please substitute for the specification the following:

Patent Application of

John H. Messing

for an

ELECTRONIC SIGNATURE METHOD

Cross References to Related Applications

None.

Background -- Field of Invention

This invention relates to creating and verifying between computers and on computer networks electronic signatures for electronic documents, filings and transaction records.

Background -- Description of Prior Art

An electronic document, legal filing or record of an electronic commercial transaction requires a way to authenticate the parties. Because handwritten signatures on paper have performed the authentication function traditionally, and electronic documents do not allow for this physical method of authentication, electronic substitutes must be found.

Until now, two principally different systems have been devised for "signing" electronic documents, but each has one or more significant drawbacks.

One such system, based upon the invention shown in U.S. Pat. 4,405,829 to Rivest et al. (1983) uses client-side digital signatures and certificates created through the technology of "asymmetric encryption." Electronic communications are signed, generally with the private key, in a two step process. First a digest of a message is created with a one way hash function, and then the hash function is encrypted using the private key. The authenticity of the message and its contents can be verified by a recipient as being authentic and sent from the signing party through testing of the message using the public key. Either an altered message or fraudulent sender will be detected by a computer possessing the proper software, the public key, and the digital certificate of the signer. If the message has been altered or the signer did not use the proper private key, the message will be detected as false. This method is useful for electronic authentication.

For more secure types of authentications, certification authorities typically check the identities of key holders and issue certificates to verify that they belong to the party who is identified as the holder of the key pair. They maintain lists of active and revoked certificates for use by relying third parties. Determination of authentication requires not only a check of the digital signature on the message, but also of the status of the certificate identifying the signer, which involves accessing the certificate authority and knowing how to check the lists of revoked and suspended certificates. The investment to create and operate a certification authority is considerable.

Private keys are susceptible to theft from the computers or devices where they are stored, and when stolen, can be used to commit fraud with virtually no detection until the certificate of the user is revoked by the certification authority with respect to that particular

corresponding public and private key pair. Private keys can also be compromised by sharing the passwords used to access them.

The creation and maintenance of the certification authority infrastructure requires a massive investment in equipment and personnel that results in a relatively high cost to the end user where suitable means are adopted by the certification authority to verify the true identity of a holder of a private key before issuance of a digital certificate to the alleged owner of the key.

Furthermore, in business and legal settings where both parties are required to electronically sign documents, filings or transaction records, digital certificates may be more secure and expensive than the realities of the transaction warrant, while in other settings, the protections may not be sufficient.

PenOp, U.S. Pat. No. 5,554,255(1994), and continuation serial number 298,991, U.S. Patent 5,647,017 (1997) and related patents cited therein, adopts a completely different approach to electronic signatures. It uses digital drawing tablets on a client machine as a basis for digitally capturing a handwritten signature, and then through software stores certain signature characteristics which identify the dynamic movements of the writer's hand as it moves the stylus on the tablet during signature creation, in addition to the image of the signature on the tablet. This stored information is then compared to a subsequently generated signature to determine if the signature is authentic. If a hash function is captured, digested, and linked to the document, this approach, like the "digital signature" approach of "asymmetric encryption" can determine any changes that have been made to the document since the signature was applied.

This "dynamic signature" approach avoids the massive infrastructure of the "public key encryption" certification authorities, and the problem of conflicting legal regimes applicable to electronic signing of documents in an international or multi-jurisdictional setting, but it requires the provision of a digital drawing tablet and stylus at each computer workstation where signature is to be accomplished, as well as the related software, which can be a significant system-wide item of cost. In addition, traditional forensic analysis

applicable to handwritten signatures does not yet apply to electronic signature analysis, and it may be some time, if ever, before the legal forensic community becomes adept at dynamic signature handwriting analysis. Because there is no way at present for expert analysis of dynamic signatures, the ability to authenticate signatures is arguable at best.

Objects and Advantages

Accordingly, several objects and advantages of the invention are to provide a new type of electronic signature that does not depend upon the massive certification authority infrastructure of digital signatures on multiple client machines based on asymmetric encryption or the hardware and software investment of dynamic signatures; further that it uses only a signature key of a server computer rather than many signature keys of many client computers, further that it automatically incorporates information about the signer and generates and affixes a date and time parameter taken from the server's clock as evidence of identity at the time of the signature; further that it eliminates the need for development of a discipline that does not yet exist, namely, the forensic science of electronic handwriting analysis; and that further allows for the use by incorporation of many types of authentication into its system, as well as others that may emerge in the future.

Still further objects and advantages will become apparent from a consideration of the ensuing description and accompanying drawings.

Summary

In accordance with the present invention, an electronic signature program is described for the creation, monitoring, and verification of an electronic signature generated by the interaction between two computers, one a client and the other a server, for the signing of documents, filings or transaction records without the need for an expensive and massive infrastructure of certification authorities and the complexities of installing and using digital certificates, without generating conflicts between applicable legal regimes in an

international or multi-jurisdictional setting over regulation of encryption software, and/or without requiring hardware tablets and associated computer software. This system further is able to incorporate other existing technologies of prior art designed to authenticate users to a server computer and ones not yet available or existing.

Drawing Figures

Fig. 1 shows authentication as a means of access by a web browser to a web server. While only certain transactions may require authentication, all users are identified at a minimum by unique network location (IP address).

Fig. 2 shows how a web server "parses" or separates out for storage certain information transmitted by a web form page.

Fig. 3 shows the creation of the signature from database submission information and the system clock.

Fig. 4 is a representation of the machine process whereby the computer takes the signature token, wraps it in a digital wrapper, and signs it with the server's private key.

Fig. 5 is a representation of a web page as shown to the user which contains the signature button for signing the document.

Description – Figs. 1 to 5

The electronic signature is affixed between computers over the Internet. Figure 1 depicts the initial contact between an Internet client user and an Internet server. This is accomplished by an ordinary web browser. Users are identified. A method for authenticating users allows the additional option to screen out unauthorized users (fig. 1, no. 12). To access the signature device, users must pass the authentication gateway. Where unauthorized users are to excluded, many different systems of screening out unauthorized

computer users can be utilized, including but not limited to digital certificates to users from trusted third parties, previously issued passwords, stored and verifiable dynamic signatures, credit card authorizations, retinal scans and other authentication methods, without limitation. Unless the system is open to all users, unauthorized users are rejected by the system using the authentication system. If the system is open, the authentication mode is universal, and all users are permitted to create electronic signatures, using identifiers only.

Information is collected from the users as shown in figure 2, (no. 14). It is transmitted for the purpose of (no. 15), parsing (separating out discrete information supplied by the user upon submission of a web page form that is specific to a filing, document or transaction)(no. 16) and storage of the information on the server computer (no. 17).

Creation of the signature is depicted in figure 3. In the preferred embodiment, the server has captured the unique network element parameter of a signer, and where available, a credit card authorization number from a card processor. Where authentication on the basis of stored identity criteria, such as a digital certificate, username and password, or biometrics is involved, alphanumeric elements, appropriate symbols or abbreviations can be used to represent these. Other user identifier elements are known to those skilled in the art and may include a legacy application that has developed a user identifier system. Certain information from the user elements (no. 18) are combined with the date-time parameters of the server's system clock (no. 19) to create a Globally Unique Identifier (GUID) from the blend of the components. (no. 20). This combination also permits a date and time stamp to be incorporated into the signature.

Figure 4 demonstrates how the GUID is encapsulated in the digital signature of the server computer. An active X (com) object or other applications programming interface (API)(no. 23) at the Internet server creates a digital wrapper (no. 24) and communicates with the signature program of the Internet server to sign the information (no. 22), including GUID, contained in the signature (no. 21) with the server's private key. Once the signature is thus encapsulated and digitally signed, it is included in an automatically generated email

message (no. 25). It is sent to the user at the email address that the user self-reported to the Internet server initially.

The digitally signed wrapper ensures that the information included in it, including GUID particulars, date and time stamp, and electronic signature cannot be altered after the fact without such change being detectable through software.

The digitally signed wrapper also permits signer-supplied submission information to be inserted into a document for signature as part of a transaction template, which may include standard terms applicable to the class of transactions. The template may simply be a blank (structure only) document, to be filled in completely by the user, or it also may include "boilerplate", meaning standardized language that is intended to remain in the document. Boilerplate is commonly associated with legal, financial, real estate and mortgage phrases and provisions that are intended as inalterable in the document finalization and signature process. For example, it can include standard terms for purchase orders. For example, it can include notices and averments to governmental regulatory bodies. For example, it can include electronic credit card charge slips. By putting the boilerplate terms and conditions at the server and incorporating them as a template that cannot be modified by a signer, unauthorized pre-signature modifications are prevented. For example, in an extreme example, the template located on the server consists completely or almost entirely of boilerplate language that the signer is expected to accept and sign or reject without adding, modifying or inserting any information specific to the signer or transaction. For example, the transaction template may be used as an envelope for the transmission and routing of one or more documents or files that are to be annexed. Any of the documents and files to be annexed can also be signed using this invention.

In a normal transaction, assuming a template consists of text *a, b, c* and more text *e, f, g* and still more text *i, j, k;* with spaces that a user fills in with transaction specific information *d* and *h*; then by way of illustrative example, the digital wrapper which is assembled for the signature at the server consists of *abc + d + efg + h + ijk + GUID.*

As one skilled in the art can appreciate, the GUID may appear in the document, in a detached signature, in a database record, in a cookie on a client user's machine or as part of the signed file information. The template can also include formatting and structuring information so that the relying party receives a document that can be read using conventional programs and methods. For example, the relying party may want to have the transaction in a word processing format. For example, the relying party may want to have the document include mark up tags common to and from such programs and languages as Hypertext Mark Up Language (HTML), Rich Text Format (RTF), Standard General Markup Language (SGML) or Extensible Markup Language (XML), and commonly used word processing formats. For example, the relying party may want to have a particular stylesheet associated with a document to preserve its layout as well as text and require the signer to sign this presentation formatting as well. By putting the templates and encryption keys on the server, and exposing the methods and properties of signature applications at the server, inconveniences caused by the complexities of using keys and certificates by non-IT professionals, and incompatibilities between operating systems and environments of the various signers' and relying parties' computers are also avoided.

Return of this information to the individual who signed the information is a receipt that is proof of the transaction, the electronic signature, and the transaction content.

If the email address is non-existent, intermediate mail server computers usually alert the server via a failed email message that the message was undeliverable. Such a message also serves to warn the server computer that a fraudulent transaction may be in progress.

Figure 5 depicts the mechanism for actually invoking the signature device, as viewed by the user. A simple button (no. 23) is clicked by the user, coupled with a clear warning (no. 24) of the consequences of clicking the signature button. Once the button is clicked, the electronic signature feature is enabled. Other means of user interaction with a machine besides the clicking of a button will be evident to one skilled in the art, and may include by way of examples a voice activated command, the pressing of a button on a keyboard, the use of a stylus or a finger on a screen, or a button on the remote control device for a television.

If the email receipt containing the electronic signature is received by the signer, that individual optionally may be required to countersign the receipt digitally (preferably using asymmetric encryption) and then to return the resigned message back to the server computer for storage and as further proof of receipt and authentication. This receipt at the server computer proves that the user actually received the electronically signed message, and the digital signature can be stored at the server as a further guarantee of message authenticity. As one skilled in the art will realize, the example of email transmission is one of many possible ways of transmitting the digitally signed document from the server to its destination. Other examples include the saving of a web page of information directly from a browser to a hard drive, or the downloading of a document from one machine to another.

Conclusions, Ramifications, and Scope

Accordingly, it can be seen that the above system allows client computer users to sign electronic documents, filings and transaction records submitted to a server computer as though with pen and ink on paper, without any additional hardware or software apart from an Internet web browser. The signature program reduces the need for a massive infrastructure investment of certification authorities by relying solely upon the digital certificate of the server computer, without any similar requirement that the signing party obtain a separate digital certificate, unless optionally required for receipt signing purposes. The method is able to make use of other current and future technologies for computer user authentication systems, and is suited for the Internet and other computer networks.

Although the description above contains much specificity, this should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. Various other embodiments and ramifications are possible within its scope. For example, other unique system information of the server can be used in addition to the system clock to generate a GUID, which may also be encrypted.

Modification within the spirit of the invention will also be apparent to those skilled in the art. For example, electronic processes may sign as client users on behalf of individuals or entities. For example, in another embodiment, the GUID may be used as the password or seed for a symmetric encryption cipher known to one skilled in the art such as RC4 to generate a unique encryption key. Application of this key to the document to be signed symmetrically encrypts the document. This encrypted version of the document is unique and constitutes the signature of the document. To verify the document, either the encrypted version is decrypted using the unique key, or the presented version for verification is re-encrypted using the unique key. If the presented document is genuine, the two end products will be identical. As the GUID contains also information about the identity of the signer, an electronic signature is created. As an intermediate step in the signature process, the document may optionally be hashed or digested prior to encryption with the symmetric cipher.

Thus the scope of the invention should be determined by the appended claims and their legal equivalents, rather than by the examples given.

Very respectfully,

John H. Messing
Postal Address: 6571 N. Silver Smith Place
Tucson, AZ 85712
Tel.: (520) 327-7750
Or (520) 529-3275
Fax: (520) 325-1087

In the United States Patent and Trademark Office

Serial Number: 09/081,872
Appn. Filed: 05/20/98
Applicant(s): John H. Messing
Appn. Title: Electronic Signature Program
Examiner: Douglas J. Meislahn
Group Art Unit: 2767

Mailed: December 28, 2000

At: Tucson, Arizona

Statement Accompanying Substitute Specification

Assistant Commissioner for Patents
Washington, District of Columbia 20231

Sir:

Attached is a substitute specification which only contains subject matter from the original specification of record, the claims and drawings, and no other new matter; together with a marked-up copy showing the amendments to be made via the substitute specification relative to the specification at the time of this filing.

Very respectfully,

John H. Messing
Postal Address:
6571 N. Silver Smith Place
Tucson, AZ 85750
U.S. Citizen
Tel.: (520) 327-7750
Or (520) 529-3275
Fax: (520) 325-1087
Email: jmessing@law-on-line.com